UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/719,193	12/08/2000	Louis Goubin	T2146-906738	5716

181 7590 08/02/2004

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
JACK, TODD M	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 08/02/2004

6

Please find below and/or attached an Office communication concerning this application or proceeding.

4

Office Action Summary	Application No.	Applicant(s)	
	09/719,193	GOUBIN ET AL.	
	Examiner	Art Unit	
	Todd M Jack	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 25 Jan 2001.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 27-45 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 27-45 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2/12-8-2000.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

Claim 33 is objected to because of the following informalities: Claim 33 possesses a mis-spelled word, "saud", on line 5 of the claim (i.e. "executing "saud" modified"). Appropriate correction is required.

Claim 33 is objected to because of the following informalities: Claim 33 possesses a mis-spelled word , "astandard", on line 2 of the claim. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 27-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Schneck (6,314,409).

Claim 27: Schneck teaches the employing of asymmetric encryption algorithms where the algorithm used for encrypting the data is associated with the key, which is encrypted

using the rule-encrypting key. The rule-encrypting key is known only to (and protected within) each receiving computer of each user. (col. 12, lines 14-28)

Claim 28: Further, Schneck teaches an inquiry to a certification database or certification authority to obtain the public key (col. 14, lines 43-61).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 29-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck (6,314,409) in view of Granger (6,480,959).

Claim 29: Schneck fails to teach that each secret key used by the cryptographic calculation corresponds to a specific piece of the secret data. Granger teaches the table decryptor decrypts the response values using the key value that was used by the table encryptor. The output of the ESD simulator is passed to the decryption engine as the key for decrypting the block of encrypted user data. Granger (col. 12, lines 29-38). Granger teaches the ESD's response value is used as the key (col. 10, lines 35-40). It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by including a secret key corresponding to a specific piece of data. This modification would have been obvious

because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to further improve the security of the system.

Claim 30: Further, Scheck fails to teach a cryptographic calculation uses nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address that is a function of the km input bits, and for each of the nonlinear transformations, the k tables are part of the secret data. Granger teaches the function of multiplying the values of a spreadsheet array by a number N integrated into the decryption code. During the encryption phase, can multiply the array by a random number R that is based on a ESD calculation. Granger (col. 12, lines 47-65) In addition, Granger teaches the use of the DES algorithm (col.. 10, lines 22-29), which is a non-linear transformation. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to increase the flexibility of the cryptographic system.

Claim 31: Further, Schneck fails to teach a cryptographic calculation process uses nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address obtained by applying a public function of the km input bits of the nonlinear transformation, and for each of the

nonlinear transformations, the k tables are part of the secret data. Granger teaches an ESD receives a 64-bit seed value and returns a 64-bit response value, this response value is generated by the ESD by applying a one-way hash function to the seed value and a 64-bit "K-value." Granger (col. 9, lines 60-67) Each of the 2^{64} possible K-values makes the hash function operate differently. Granger (col. 10, lines 1-7) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by applying a function to a value and obtaining a transformation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to operate more efficiently on the value.

Claim 32: Further, Schneck fails to teach storing a conversion table calculation program in each computer system and activating the calculation program by a given event in order to calculate tables and store all or part of the tables in secret data. Granger teaches a block of user data is encrypted to produce an encrypted block of user data. The block of user data may consist of the first 64 bytes of a file that is being written to mass storage, or may be a table entry that is being written to RAM. Granger (col. 10, lines 15-21) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by storing a conversion table calculation program and activating the calculation program by a given event. This modification would have been obvious because a person having ordinary skill in the art

would have been motivated to do so, as suggested by Granger, in order to maintain a number of the variables for system operations.

Claim 33: Schneck teaches an inquiry to a certification database or certification authority to obtain the public key (col. 14, lines 43-61). This corresponds to storing a modified algorithm that adheres to computational phases of a standard cryptographic algorithm. Schneck fails to teach storing a modified cryptographic algorithm that adheres to computational phases of a standard cryptographic algorithm, a secret encryption key contained in a secret area of the storage means for modifying the standard cryptographic algorithm, means for executing said modified cryptographic algorithm, first secret means for replacing intermediate variables required for the computational phases of the standard algorithm with a plurality of partial intermediate variables, second means for applying a nonlinear transformation table to each of the partial intermediate variables, and third secret means for reconstituting a final result corresponding to utilization of the standard cryptographic algorithm from results obtained on the partial variables. Granger teaches, respectively, the encryption engine applies a key-based encryption algorithm to the block of user data (col. 10, lines 22-25), replacing the code which queries the ESD with a piece of code that always returns the same 64-bit response value (col. 11, 1-4), adding code which implements the ESD's number calculation algorithm (col. 11, lines 12-21), and a number calculation algorithm of the ESD resulting from the encrypted look-up table of seed response pairs (col. 11, lines 23-30). During the decryption phase the seed value is similarly passed to a

condenser, the output of the condenser is passed as a look-up table index to the ESD simulator, the ESD simulator uses this value to retrieve the response value from the look-up table, decrypts the response value using a table decryptor, the table decryptor decrypts the response value using the key value, and the output of the ESD simulator is passed to the decryption engine as the key for decrypting the block of encrypted user data (col. 12, lines 26-38). The look-up table acts as a non-linear table to provide the key necessary to decrypt the intermediate variables, which are the block of encrypted user data. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a secret encryption key, executing the modified cryptographic algorithm, means for replacing intermediate variables, means for applying a nonlinear transformation table, and means for reconstituting a final result. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to alter the cryptographic algorithm as needed to ensure the continued security of the computer system.

Claim 34: Further, Schneck teaches cryptographic variables (e.g., keys) and clear text information as a protected data set (col. 21, lines 35-64) and computing a hash function of the data (col. 21, lines 34-36).

Claim 35: Further, Schneck fails to teach a modified cryptographic algorithm includes tables used for applying the nonlinear transformations to the partial variables, at least

one of the tables, formed by random selection, and being stored in the secret data, the other tables required for the calculations being stored in a nonvolatile memory, means for executing various computational rounds of the standard algorithm, each time using the tables on the partial variables, and means for calculating the result in the last round of the algorithm by combining the partial variables in accordance with a second secret function. Granger teaches the generation of tables storing variables, constants, and other entities using the mapping library's operations (col. 20, lines 21-45), during each iteration of the process a machine-level instruction for which an obfuscation rule exists is selected at random (col. 21, lines 39-42), and a code input to a function to be chosen by random (col. 22, lines 60-67). It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by applying tables with modified algorithms, storing the data, and calculating results. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to modify the cryptographic processing of the data, thus enhancing the protection of the tables.

Claim 36: Further, Schneck fails to teach the modified algorithm are constituted by a function, linking the partial intermediate variables and each intermediate variable, such that the knowledge of one value of the intermediate variable never makes it possible to deduce all of the particular partial values such that there exists a tuple that satisfies the equation. Granger teaches an ESD receives a 64-bit seed value and returns a 64-bit

response value is used. The response value is generated by the ESD by applying a one-way hash function to the seed value and K-value. K-values make the hash function operate differently where knowledge of the hash function does not compromise security. Granger (col. 9, lines 60-67 and col. 10, lines 1-7). It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by modifying the algorithm by a function linking the variables. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to assure that the loss of privacy does not represent a breach in the security of the system.

Claim 37: Further, Schneck fails to teach the second means of the modified algorithm are constituted by k partial conversion tables, and among the k partial conversion tables, k-1 partial conversion tables contain secret random variable. Granger teaches the function of multiplying the values of a spreadsheet array by a number N integrated into the decryption code. During the encryption phase, can multiply the array by a random number R that is based on an ESD calculation. Granger (col. 12, lines 47-65) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to

enhance the security of the process by making available randomly chosen variables for the use in calculations.

Claim 38: Further, Schneck fails to teach the second means of the modified algorithm comprise conversion tables, each of the conversion tables receiving an input a value obtained by applying a secret bijective function to the function of the partial intermediate variables in accordance with the relation, this application being performed by direct evaluation of a resulting value, this resulting value, applied to the input of the conversion table, making it possible to read n output bits of the transformation at an address that is a function of these m input bits. Granger teaches an ESD receives a 64-bit seed value and returns a 64-bit response value; this response value is generated by the ESD by applying a one-way hash function to the seed value and a 64-bit "K-value." Granger (col. 9, lines 60-67) Each of the 2^{64} possible K-values makes the hash function operate differently. (col. 10, lines 1-7) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by applying a function to a value and obtaining a transformation. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to read output bits of the transformation at an address that is a function of these input bits.

Claim 39: Further, Schneck fails to teach a modified algorithm comprise means for replacing each nonlinear transformation applied to an intermediate variable of the

standard cryptographic calculation process, without a separation with a partial nonlinear transformation of km bits into kn bits applied to all of the partial intermediate variables, means for calculating of the output bits of this transformation as a polynomial function of the km input bits, and means for reading the remaining n bits are read at an address that is a function of the km input bits. Granger teaches replacing the code, which queries the ESD with a piece of code that always returns the same 64-bit response value (col. 11, 1-4), the function of multiplying the values of a spreadsheet array by a number N integrated into the decryption code. During the encryption phase, can multiply the array by a random number R that is based on an ESD calculation. Granger (col. 12, lines 47-65). Granger teaches the function of multiplying the values of a spreadsheet array by a number N integrated into the decryption code. During the encryption phase, can multiply the array by a random number R that is based on an ESD calculation. Granger (col. 12, lines 47-65) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to alter the encryption/decryption process with the attempt to increase the security of the system.

Claim 40: Further, Schneck fails to teach a means for sequentially executing operations performed by the modified algorithm in the various parts resulting from the separation of

the cryptographic calculations process into several distinct calculation process parts. Granger teaches the addition of the ESD simulator to the application can be accomplished by adding code, which implements the number calculation algorithm. An encrypted look-up table of seed-response pairs will be used. Granger (col. 11, lines 1-4, lines 12-21, and lines 23-50) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to enhance the speed of the processing.

Claim 41: Further, Schneck fails to teach a means for executing, in interleaved fashion, operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts. Granger teaches the addition of the ESD simulator to the application can be accomplished by adding code, which implements the number calculation algorithm. An encrypted look-up table of seed-response pairs will be used. Granger (col. 11, lines 1-4, lines 12-21, and lines 23-50) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to increase the rate at which the calculations are performed.

Claim 42: Further, Schneck fails to teach a means for simultaneous executing operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts, in the event of multiprogramming. Granger teaches the addition of the ESD simulator to the application can be accomplished by adding code, which implements the number calculation algorithm. An encrypted look-up table of seed-response pairs will be used. Granger (col. 11, lines 1-4, lines 12-21, and lines 23-50) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to allow for the increased speed and responsiveness of the system created by multiprocessing.

Claim 43: Further, Schneck fails to teach a means for simultaneously executing, in different processors working in parallel, the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts. Granger teaches the addition of the ESD simulator to the application can be accomplished by adding code, which implements the number

calculation algorithm. An encrypted look-up table of seed-response pairs will be used. Granger (col. 11, lines 1-4, lines 12-21, and lines 23-50) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by using a cryptographic calculation described by conversion tables where the tables are part of the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to utilize the increased speed of calculating and responsiveness.

Claim 44: Further, Schneck fails to teach including a conversion table calculation program stored in each computer system and means for activation by a given event of the calculation of the tables and for the storage of all or part of these tables in the secret data. Granger teaches a response value is generated by the ESD by applying a one-way hash function to the seed value and a 64-bit K-value. The K-value is programmed into the ESDs by the software developer prior to shipping the ESDs to customer, and is maintained in secrecy by the software developer. The K-value makes the hash value operate differently. The block of data may consist of the first 64 bytes of a file that is being written to mass storage, or may be a table entry that is being written to RAM. Granger (col. 9, lines 65-67 and col. 10, lines 1-21) It would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Schneck by storing a conversion table calculation program stored in each computer system and means for activation by a given event of the calculation of the

tables and for the storage of all or part of these tables in the secret data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to prevent unauthorized access to the tables and their entries.

Claim 45: Further, Schneck fails to teach a counter having means for storing a value that is incremented with each cryptographic calculation so as to constitute a given for the activation, by activating means, of the calculation of the tables when a given value is exceeded. Granger teaches the PC is incremented by one to point to the next line of the data block. The PC is loaded with an immediate value specified within the instruction. This value produces the processing of branch and jump instructions. Granger (col. 19, lines 14-18) This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Granger, in order to ensure that there is sufficient space to store a value by monitoring the number of events versus those events that can be possibly stored.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 703-305-1027. The examiner can normally be reached on M-The.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decay, can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack
Art unit 2133

July 15, 2004

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100